Zero Data Loss Recovery Appliance

Oracle Zero Data Loss Recovery Appliance RA26

今日のデータ保護ソリューションを使用して、ミッション・クリティカルな企業データベースのニーズを満たすことは簡単ではありません。これらのソリューションでは、リストアのたびに最大で1日分のビジネス・データを失う可能性があり、データベース・レベルのリカバリ可能性を検証する機能に欠け、フルバックアップ中の本番サーバーには高い負荷がかかります。これらの課題のおもな原因は、データベースを特定の整合性とリカバリの要件のあるトランザクション・システムとして処理せず、基本的に一連の分散ファイルとしてコピーするという処理方法を利用しているためです。ランサムウェア攻撃に直面すると、ビジネスへの影響はさらに深刻化します。ランサムウェア攻撃によって、検知されることなく本番データとバックアップ・データの両方が侵害され、企業のデータとリカバリ可能性が人質に取られる可能性があります。

オラクルのZero Data Loss Recovery Appliance（Recovery Appliance：RA）は、Oracle AI Databaseと緊密に統合して、これらの要件に真っ向から対処する革新的なデータ保護ソリューションです。データ損失を排除し、リカバリを高速化し、本番サーバーへのデータ保護のオーバーヘッドを激減させます。さらに、Recovery Applianceはサイバー・レジリエンスを確保するためのバックアップ・データの整合性とリカバリ可能性を継続的に検証し、数千ものデータベースを保護するために拡張可能で、ライフサイクル全体を通じてディスク・バックアップ、リモート・レプリケーション、クラウド・アーカイブを含めバックアップを保護します。

今日のデータベース保護の課題

今日のデータベース保護ソリューションの根本的な課題は次のとおりです。

- バックアップ方法とリカバリ方法が旧来の夜間バックアップ・パラダイムに基づいており、最大で1日分の貴重なデータをリストアごとに失う可能性があるため、アプリケーション間のトランザクション一貫性とビジネスのSLAに重大な影響が及ぶ
- バックアップ中、データの変更の有無に関係なく、データベースの全データを処理することで、本番サーバーとネットワークにバックアップの大きなオーバーヘッドがかかるため、アプリケーションのパフォーマンスが低下する可能性がある

おもな機能

- リアルタイムのREDO転送
- エンド・ツー・エンドのデータ検証
- 永久増分バックアップ戦略
- 省スペースの暗号化された仮想フルバックアップ
- バックアップ操作のオフロード
- データベース・レベルの保護ポリシー
- データベース対応の領域管理
- クラウド規模のアーキテクチャ
- 効率的なレプリケーション
- クラウド/ZFSへのポリシー駆動型アーカイブ
- 統合された管理と制御
- ラックあたり最大1.9 PBのバックアップ容量
- ラックあたり最大60 TB/時のバックアップおよびリストア・スループット

- 絶え間ないデータ増加によってバックアップ・ウィンドウがますます拡大するため、データ損失のリスクにさらされる時間が長くなり、運用ワークロード期間への影響が増大する
- バックアップ・アプライアンス機器では拡張によりデータセンターの数百から数千のデータベースを保護できないため、“ITのスプロール化”が無秩序に発生し、デプロイメントおよびメンテナンスのためのコストが過大になる
- Disk-to-Disk-to-Tapeやレプリケーションを含むデータ保護ライフサイクル全体を十分に可視化し制御することができないため、レポート作成やリカバリに欠落が生じる可能性がある

Zero Data Loss Recovery Applianceの紹介

Oracle Zero Data Loss Recovery Appliance（Recovery Appliance）は、特にデータベースを保護するように設計された世界初のエンジニアド・システムです。

Recovery Applianceはすべてのデータベースを継続的に保護しながら、すべてのバックアップ処理においてオフロードを実現し、本番サーバーにおけるオーバーヘッドを最小限に抑えます。

このアプライアンスは、ベース・ラック構成で開始して小規模Oracle環境に対応でき、そこからスケールアウトして、データセンターの数百から数千のデータベースのデータ保護要件をサポートできます。

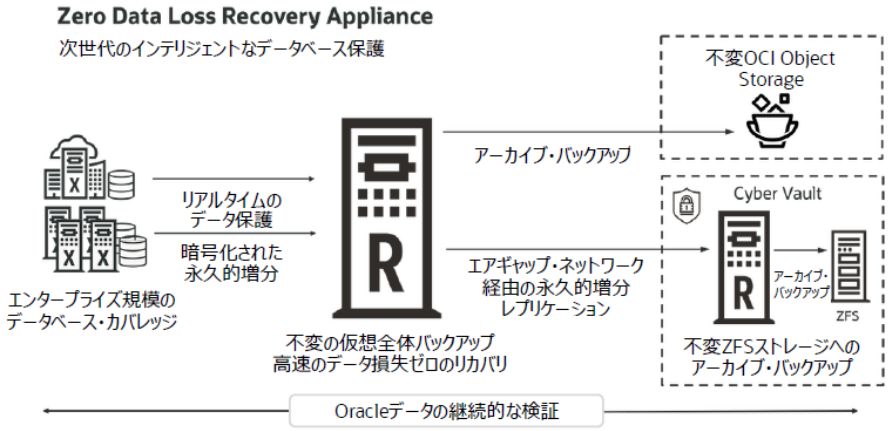

図1：Zero Data Loss Recovery Appliance：アーキテクチャ概要

Recovery ApplianceはOracle AI DatabaseおよびRecovery Manager（RMAN）と緊密に統合して、他のデータ保護ソリューションでは提供できないデータ保護機能とパフォーマンスを実現します。

おもな利点

- データ損失の排除
- 高速で最適化されたリカバリ
- 最小限の影響しか及ぼさないバックアップ
- データベース・レベルのリカバリ可能性
- クラウドへの統合アーカイブ
- クラウドスケールの容量とパフォーマンス

Recovery Applianceのおもな設計目標は、既存のデータ保護ソリューションでは失われる恐れのある重要なデータベース・データの損失をなくすことです。

「当社はデータ・ドメインをオラクルのZero Data Loss Recovery Applianceに換えて、リアルタイムの増分バックアップとリストアを、月額8億5千万米ドル超のクレジットカード取引データに対して、データ損失なく実現しています。また、平均バックアップ・サイズが30分の1に減少し、バックアップ容量が65 %増えました。」
KEB Hana Card
ITチーム、シニア・マネージャー
Iljoon Lee氏

データ損失の排除

Recovery Applianceは、処理中のOracle AI Databaseトランザクションを保護することにより、コスト効率の良い方法でデータ損失のリスクを最小限に抑えるように設計されています。これは、汎用バックアップ・ソリューションでは実現できません。

リアルタイムのREDO転送

REDOログは、Oracle AI Database内でトランザクションによる変更を実装する基本的な手段です。Oracle Database 19cおよびそれ以降のバージョンのデータベースはすべて、インメモリ・ログ・バッファからREDOを継続的にRecovery Applianceに直送できます。これにより、独自のリアルタイムのデータ保護が実現して、データベースを最後の1秒未満まで保護できます。REDOはデータベース共有メモリから送信されるため、本番システムへのオーバーヘッドが極めて低くなります。

リアルタイムのREDO転送はオラクルのData Guardテクノロジーに初めて実装され、世界中の数千ものミッション・クリティカルなデータベースで導入されています。Recovery Applianceはこのテクノロジーをシンプルにコスト効率よく最上位層以外のデータベースにまで拡張します。Recovery Applianceは、Data Guardの高速フェイルオーバーと問合せオフロード機能を必ずしも必要としないデータベースに対し、今日のData Guardと同様のレベルのデータ保護を実現します。

効率的なレプリケーション

ローカルRecovery Appliance上のバックアップは、サイトの停止や地域の災害からの保護対策として、リモートRecovery Applianceに簡単に素早く複製できます。レプリケーション・トポロジは、データセンターの要件に合わせてカスタマイズできます。たとえば、レプリケーションをシンプルな1方向のトポロジに設定したり、2台のRecovery Applianceを相互のレプリケーションに対応できるように設定したり、中央のRecovery Applianceへのレプリケーションが可能になるように複数のサテライトRecovery Applianceを設定したりすることができます。ローカルRecovery Applianceを使用できない場合、データをローカルでステージングしなくても、リストア操作をリモートRecovery Applianceから直接実行できます。

Recovery Applianceを使用すると、企業はクラウド・ストレージの利用をオフサイトの安全な保護層として拡張できます。

アプライアンスは"Backup Anywhere"ペア・レプリケーション構成でセットアップすることもでき、その場合は一方のシステムに取られたバックアップが他方のシステムに自動的に同期されます。これにより、どちらかのシステムに影響を与える障害が発生した場合でも、バックアップとリカバリ操作のための高可用性を維持できます。

すべてのトポロジで、変更されたブロックだけが複製されるので、WANネットワークの使用を最小限に抑えられます。

クラウド/ZFSへのポリシー駆動型アーカイブ

Oracle Cloudとの統合により、低コストのオフサイト・ストレージに直接アクセスできます。これにより、物理メディアの紛失やオフサイトへの送付忘れなど、物理メディアの移動に伴うリスクが軽減されます。また、物理メディアの到着を待つ必要がないため、必要なときに、はるかに早くリカバリ・プロセスを開始できます。

オンプレミスのバックアップ・アーカイブが必要なお客様のために、Recovery Applianceは、ZFS OCIオブジェクト・ストレージ・インタフェースとの統合により、Oracle ZFS Storageへのフル・バックアップと増分バックアップをオフロードします。

アーカイブとリストア操作は、ZFSとの間で直接25 Gbまたは100 Gb接続で実行できます。

あるいは、他のベンダーのメディア管理バックアップ・エージェントをRecovery Applianceにデプロイして、既存のバックアップ・インフラストラクチャ、メディア・サーバー、プロセスに統合することもできます。

アーカイブ・プロセスは、Recovery Applianceに完全にオフロードされ、本番データベースからこれらのバックアップを作成する影響は排除されます。従来の週次フルおよび日次増分アーカイブ戦略は、拡張リカバリ・ウィンドウの要件を満たすために採用でき、ポイントインタイム・アーカイブ・バックアップ（RMAN KEEPバックアップに類似）は、数か月または数年のコンプライアンス保持要件を満たすために作成できます。アーカイブ操作はアプライアンスから1日中実行でき、本番システムの速度を低下させることなく、リソース使用率の向上とコスト削減を可能にします。

確実なリカバリ：エンド・ツー・エンドのデータ検証

すべてのバックアップ・データとREDOブロックが、バックアップ・ライフサイクルの各ステージで自動的に個別に検証されます。

Recovery ApplianceはOracle AI Database内部のブロック形式を認識し、深いレベルのデータ検証を実現します。バックアップ・データとREDOブロックはすべて、Recovery Applianceで受信されたとき、クラウドにコピーされたとき、複製されたときに自動的に検証されます。また、バックアップ・ブロックは定期的にディスク上で検証されます。これにより、リカバリ操作の成功率が大幅に向上します。これは、Recovery Applianceの深いデータベースとの統合がないと実現しないもう1つの独自の差別化要因です。検証中に破損が検出されると、Recovery Applianceを支えるストレージ・ソフトウェアによって、ミラー・コピーから正常なブロックが自動的に読み取られて、破損したブロックが即座に修復されます。

さらに、Recovery Applianceストレージ・ソフトウェアは、基盤のハード・ディスクを定期的に検査します。不良セクターが検出されると、ミラー・コピーから即座に修復され、これはユーザーに対して完全に透過的に行われます。

最小限の影響しか及ぼさないバックアップ

24時間365日体制の要件があっても、多くの企業は依然として数時間のバックアップ・ウィンドウを設ける必要があり、その間本番アプリケーションのパフォーマンスが影響を受ける場合があります。バックアップ・ウィンドウはビジネスのメリットに直結せず、ピーク時間以外の処理時間をめぐってビジネスに不可欠なレポーティングおよびバッチ・ワークロードと時間を争奪し合う事態を招いています。グローバル経済が成長する中、バックアップ・ウィンドウは縮小し続けていますが、データ量は増大しています。

現在のディスクベースのデータ保護ソリューションの影響

現在のディスクベースのデータ保護ソリューションは、本番システムに大きな負荷を課しています。データベースが拡大し続ける中、この影響はこれからも大きくなります。おもな課題のいくつかを以下に挙げます。

- 重複排除アプライアンスは定期的にフルバックアップを取得する必要があります。フルバックアップではデータベース全体が読み取られるため、本番ストレージ、サーバー、ネットワークに大きな影響が及ぶ上に、長時間のバックアップ・ウィンドウを不必要に設ける必要があります。

- ソース側の重複排除を使ってネットワーク要件を軽減する場合、本番サーバーに高いCPUとメモリの負荷がかかるという悪影響が生じます。
- リカバリ・フェーズの間、データベースを開く前に、増分バックアップをリストア済みのデータファイルに適用する必要があります。このプロセスでは、増分の変更適用に数日間かかることがあり、適用操作は通常、ネットワークを通して実行されるため、リカバリに非常に長い時間を要すことがあります。

永久増分バックアップ・アーキテクチャ

Recovery Applianceの2つ目の基本的な設計戦略は、本番データベース・システムでのバックアップ関連の処理を可能な限り最小限に減らして、変更データだけを送信することです。不要なバックアップ処理の排除により、本番システムはおもな目標である、ビジネスに不可欠なワークロードの処理に集中できるようになります。

Recovery Applianceは永久増分バックアップ・アーキテクチャを実装して、本番システムへの影響を最小限に抑えます。このアーキテクチャは、次の2つの革新的なテクノロジーをベースにしています。それは、Delta PushとDelta Storeです。

Recovery Applianceを使用すると、本番データベース・サーバーは、本番ワークロードを処理する本来の仕事に専念でき、バックアップやリカバリのタスクに忙殺されることがなくなります。

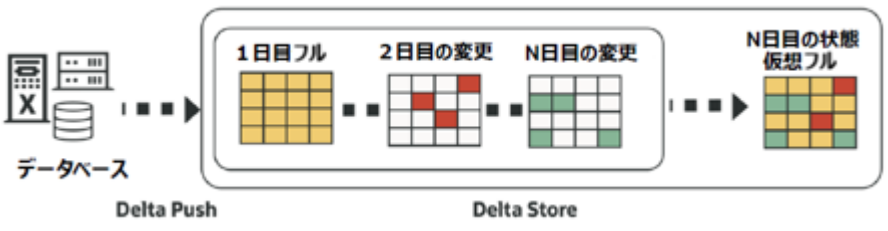

図2：Zero Data Loss Recovery Appliance：Delta PushとDelta Store

Delta Push

Delta Pushを使用すると、保護されたデータベースは、そのデータベースに加えられた変更のみ含む増分バックアップだけをRecovery Applianceに送信します。定期的なフルバックアップのスケジュール設定や実行の必要はありません。Delta Pushは"永久増分"としても知られています。1回のフルバックアップ以後は、増分バックアップだけが本番システムで実行されるためです。Delta Pushは実質的に、ソース側の重複排除を高度に最適化したものです。

Recovery Managerのブロック・チェンジ・トラッキングを使用すると、本番データベース上の変更されたブロックが非常に効率的に識別されるため、変更されていないデータを読み取る必要がなくなります。

保護されたデータベースとRecovery Appliance間の特別な統合により、コミットされたUNDO表領域、未使用の表領域、ドロップされた表領域ブロックがバックアップ・ストリームから排除されて、オーバーヘッドと領域の消費が大幅に減ります。

Delta Pushは、フルバックアップではなく変更されたデータだけを送信するので、他のソリューションに比べてネットワーク・トラフィックが大幅に軽減されます。これにより、低コストなイーサネットをバックアップに使用できます。また、ネットワーク・トラフィックを最小限に減らすことで、保護されたデータベースからさらに遠くにRecovery Applianceを配置でき、場合によってはWAN越しのリモート・データセンターに配置できます。

Delta Store

Delta StoreはRecovery Applianceソフトウェア・エンジンの"ブレイン"です。Delta Storeは、変更されやって来るデータ・ブロックを検証してから圧縮し、索引を付けて保存します。受信した変更データ・ブロックは、**仮想データベース・フルバックアップ**の基盤となるものであり、仮想データベースフルバックアップは、増分バックアップのポイント・イン・タイムにおけるスペース効率に優れた物理フルバックアップのポインタベースの表現です。仮想フルバックアップは、データセットおよび保護されたデータベースの変更率に応じて10倍以上ストレージを効率化できます。

たとえば、100 TBのデータベース、1 %の変更率、30日のリカバリ期間ポリシーの場合、従来どおりにフルバックアップを毎週、増分バックアップを毎日実行する手法だと、次のような結果になります。

- フルバックアップ：（100 TB×5回のバックアップ）
- 増分バックアップ：（1 TB×30回のバックアップ）
- 合計：530 TB[1]

これと比較してRecovery Applianceの場合は、次のような結果になります。

- フルバックアップ：100 TB
- 増分バックアップ：（1 TB×29回のバックアップ）
- 合計：129 TB

従来のバックアップよりもストレージ消費量をほぼ5倍節約できます。Recovery Applianceのオンディスク圧縮を考慮すると、合計節約量は10倍以上に達する可能性があります。

Delta Storeアーキテクチャの劇的な領域効率により、大量の仮想フルバックアップをオンラインに維持することができ、ディスクベースのリカバリ期間を大きく広げることができます。

リストア操作が必要な場合、Delta Storeはもっとも近い増分バックアップの時間に基づいて、効率的に物理フルバックアップを再作成します。リストア操作は、Recovery Applianceの基盤となるハードウェア・アーキテクチャの大規模なスケーラビリティとパフォーマンスによってサポートされています。

Recovery Applianceからリストアする場合、従来のフルバックアップをリストアした後に、すべての関連増分バックアップをリストアおよび適用する低速プロセスが排除されます。Recovery Applianceによるリストア・パフォーマンスはより予測しやすく、SLAを満たすのに役立ちます。

リストアの高速化は、（1）データベースのテスト/開発のリフレッシュの高速化、および（2）レガシーOSプラットフォームからOracle Exadataなどの最新プラットフォームへの移行の高速化も意味します。Recovery Applianceは、革新的な仮想フルリストア・テクノロジーに基づき、最小限のダウンタイム、クロスプラットフォーム、クロスバージョンのデータベース移行作業に活用できます。

「オラクルのZero Data Loss Recovery Applianceは頼りになり、とても安心です。かつてはリフレッシュ・タスクに多くの時間を費やしていましたが、今ではDBAチームの生産性が大幅に向上し、Enterprise Managerによっていつでも制御下のOracleデータベースを保護し、緊急のリストアが必要な場合でも、非常に素早く実行して、最新のトランザクションまでリストアできるという確信が持てるようになりました。」

Evergy
リード・データベース・アーキテクト
Nazrul Islam氏

[1] 'R'日のポイント・イン・タイム・リカバリ期間ポリシーを維持する毎週のフルバックアップと毎日の増分バックアップ手法で、合計'R + 7'日間のバックアップをストレージに保持するには、さらに7日間のバックアップ（1日のフルバックアップ + 6日の増分バックアップ）が必要です。これはデータベース・リカバリ設計が原因です。このリカバリ設計では、*R*日以上経過したフルバックアップを少なくとも1つ、リストア操作のために保持する必要があり、その後、増分バックアップとアーカイブ・ログ・バックアップを使って、R日のリカバリ期間の開始時点へとさかのぼってリカバリされます。

ほとんどのバックアップ操作をオフロード

バックアップ関連の処理は実質的にすべて、Recovery Applianceにオフロードされます。これには、時間のかかる圧縮、バックアップの削除、検証、保守操作が含まれます。その結果、バックアップ・ウィンドウ外のときでも本番システムのリソースが解放されて、本番システムのパフォーマンスが向上します。

つまり、リアルタイムのREDO転送とDelta Pushにより、保護されたデータベースは最小限のバックアップ関連作業を実行し、変更されたデータだけをRecovery Applianceに送信します。クラウド・バックアップなど他のすべてのバックアップおよびリカバリ関連の処理はRecovery Applianceによって実行されます。これは、Recovery Applianceの主要なアーキテクチャ・イノベーションの1つであり、今日のバックアップ・ソリューションをはるかに超えます。

「シームレスで信頼性の高い通信サービスと金融サービスを提供するというSafaricomの約束は、Oracle ExadataとOracle Recovery Applianceの比類ないパフォーマンスとデータ保護機能によって支えられています。業界をリードするこれらのソリューションにより、優れたカスタマー・エクスペリエンスを提供し、貴重なデータ資産の最大限のセキュリティと整合性を確保することができています。」

Safaricom PLCITインフラストラクチャ/エンタープライズ
部門責任者
Mark Oyier氏

Database Protection as a Private Cloud Service（プライベート・クラウド・サービスとしてのデータベース保護）

Recovery Applianceの3つ目の設計戦略は、データセンターの数十から数千のデータベースを効率的に保護できるように、クラウド規模のデータベース保護サービスを提供することです。複数のRecovery Applianceのテクノロジーがこの目標を実現します。

ポリシー・ベースのデータ保護管理

Recovery Applianceは保護ポリシーの概念を導入して、アプライアンスとクラウド上でデータベースごとに達成するリカバリ目標を定義します。保護ポリシーを使用することで、データベースをリカバリ・サービスで階層化し容易にグループ化することができます。Recovery Applianceには事前定義済みの“Platinum”、“Gold”、“Silver”、“Bronze”のポリシーがあり、これらをカスタマイズしてさまざまなビジネス上のSLAをサポートできます。たとえば、Goldポリシーのデータベース・バックアップはローカル Recovery Appliance上で35日、クラウド上で90日のリカバリ期間を目標とし、Silverポリシーで管理されるバックアップはローカルRecovery Appliance上で10日、クラウド上で30日のリカバリ期間を目標としています。階層化保護ポリシーは、リモートへ複製されたRecovery Applianceにも個別に適用できます。

Recovery Applianceを使用すると、データ保護のレベルをアプリケーションのビジネスの重要度にはるかに的確に合わせることができ、物理的なビットとバイトのレベルに制限されることがありません。

追加のデータベースを作成した場合、既存の保護ポリシーの1つに容易に追加できます。たとえば、新しいFinanceデータベースをGold保護ポリシーに容易に追加できます。追加後、ポリシーのリカバリ期間目標が自動的にこのデータベースのバックアップに適用されます。この自動ポリシー・ベースのフレームワークにより、企業は社内全体でDatabase Protection as a Serviceを簡単に実装できます。

データベース対応の領域管理

Recovery Applianceは保護ポリシーをベースに使用しながら、各データベースのリカバリ期間目標に応じてすべてのバックアップ・ストレージ領域をフルに管理します。たとえば、Goldポリシーのメンバーである“Finance Database”は過去35日以内にリカバリできる一方で、Silverポリシーのメンバーである“Products Database”は過去10日以内にリカバリできます。Delta Storeに空き領域がある場合、リカバリ期間目標より古いバックアップが保持されて、実質的にリカバリ期間が延長されます。

ストレージ領域にあまり余裕がない場合、Recovery Applianceはバックアップを消去し、データベース間で領域を自動的に再プロビジョニングして、保護されたそれぞれのデータベースのリカバリ・ウィンドウ目標を満たします。また、すべてのデータベースのリカバリ・ウィンドウ目標を満たすために、領域が少なくなる前に、領域の使用履歴を基にバックアップを先見的に消去することもできます。データファイル、REDOログ、制御ファイル間の依存関係を認識した上で、領域はデータベース内でインテリジェントに消去されます。

このリカバリ・ウィンドウ指向の領域管理手法は、通常の汎用バックアップ・アプライアンスのように不明瞭なストレージボリューム・レベルで領域を管理しなければならない必要性を排除します。この革新的な手法では、各アプリケーションのビジネスの重要度に合わせてデータが保護され、手動による領域のリバランシングから解放されます。

クラウド規模にスケールできるアーキテクチャ

Recovery ApplianceはOracle Exadataアーキテクチャをベースにしているため、その実証済みのスケーラビリティ、冗長性、パフォーマンスを継承しています。Recovery Applianceによって保護される社内のデータベース追加に合わせて、コンピューティング・サーバーとストレージ・サーバーをアプライアンスに容易に追加できます。その結果、ビジネスの成長をシームレスにサポートする、シンプル、無停止のスケールアウト・データ保護クラウドが実現します。

「Recovery Applianceにより、バックアップの構成時間は数週間かかっていたところが5分に短縮でき、バックアップ量も40 %削減できました。」

Swisscom
ヘッド・アーキテクト
Christoph Lutz氏

Recovery Applianceの構成

ベース・ラックおよびフル・ラック構成

Recovery Appliance RA26の基本ラック構成では、100 Gb/秒のRemote Direct Memory Access（RDMA） over Converged Ethernet（RoCE）を使って2台のコンピューティング・サーバーと3台のストレージ・サーバーが内部接続されています。RoCEはクラウド規模の超高速ネットワーク・ファブリックの最新世代であり、あるコンピュータがオペレーティング・システムやCPUを介さずに別のコンピュータのデータに直接アクセスできるため、高帯域幅で待機時間の短いアクセスが可能になります。

「Recovery ApplianceはData Protection as a Service（DPaaS）を提供し、データベースのパフォーマンスを加速化し、非常に細かいレベルの粒度でリカバリすることを可能にします。」

Enterprise Strategy Group
上級アナリスト
Jason Buffington氏
プラクティス・ディレクターおよび上級アナリスト
Mark Peters氏
調査アナリスト
Monya Keane氏

RA26ベース・ラックでは、受信バックアップ用に332 TBの使用可能容量が提供されます。ベース・ラックは、RA26ストレージ・サーバーをラックに追加することで段階的にアップグレードでき、最大17台のストレージ・サーバーをフル・ラックに収納できます。各ストレージ・サーバーにより、使用可能な容量が112 TB増えます。RA26フル・ラックの使用可能な総容量は1.9 PBで、**仮想フルバックアップの**有効容量は最大***19*ペタバイト**になります。[2]

RA26-Zベース・ラックの使用可能な容量は164 TBで、RA26-Zストレージ・サーバーをラックに追加することで段階的にアップグレードでき、最大17台のストレージ・サーバーをフル・ラックに収納できます。各ストレージ・サーバーにより、使用可能な容量が56 TB増えます。RA26-Zフル・ラックの使用可能な総容量は943 TBで、**仮想フルバックアップの**有効容量は最大***9.4*ペタバイト**になります。[2]

Recovery Applianceは、通常10日間のリカバリ期間にわたって、アプライアンスの使用可能な容量とほぼ同じ合計サイズのデータベースを保護できます。たとえば、17台のストレージ・サーバーを収納し、使用可能な容量が1.9 PBのRA26フル・ラック構成では、約1.9 PBのソース・データベースを10日間のリカバリ期間の間保護することができ、その10日間で生成された10個の1.9 PBの仮想フルバックアップおよびすべてのREDOデータを保存できます。

[2] 有効容量は、毎日の変更率10 %に基づいて計算されます。

Recovery Applianceの正確なサイジングは、初期データベースのサイズと増加率、TEMPとUNDOで消費されるストレージ、空き領域、データベースの変更率、REDO生成率、目的のリカバリ期間、データベースの圧縮性など、保護されたデータベースに関わる複数の要因によります。

Zero Data Loss Recovery Applianceを使用すると、完全にスケールアウト可能なストレージとコンピューティング・サーバーで容量とスループットを拡張できます。

完全なスケールアウト・アーキテクチャ

フル・ラックを超える追加容量が必要な場合は、2台目のベース・ラックを100 Gb/秒RoCE経由で最初のラックに接続できます。2台目のラックにも、2台のコンピューティング・サーバーが収容されており、構成の接続性と処理能力を強化します。最初のラックと同様に、ストレージ容量はストレージ・サーバーの段階的な追加によって容易に拡張できます。最大14台で完全に構成されたRA26ラックを単一アプライアンスにまとめて接続して、26.6 PBの使用可能な容量、つまり、***266ペタバイトの仮想フルバックアップ***を実現できます。

Recovery Appliance RA26は単一のフル・ラックで最大**19ペタバイトの仮想フルバックアップ**を、14台のフル・ラック最大構成で**266ペタバイト以上の仮想フルバックアップ**をサポートできます。

Recovery Applianceスケールアウト・アーキテクチャのパワーと柔軟性は、追加のデータベース群をサポートする必要がある場合、またはビジネス・データが増加する場合に役立ちます。ストレージ、コンピューティング、ネットワークの容量をバランスよく段階的に追加することで、高いパフォーマンスが維持されます。従来のバックアップ・アプライアンスは通常、2台のコントローラに制限されていて、ストレージ、ネットワーク、コンピューティングをボトルネックのないバランスの取れた方法でスケーリングできないため、このアーキテクチャの方がはるかに優れています。

パフォーマンス特性

スループットが極めて高いコンピューティング、ネットワーク、ストレージの組合せとRecovery Applianceに固有のデータベースとの統合により、データセンター全体のデータ保護のニーズを容易にサポートするパフォーマンス・レベルが実現します。

単一のRecovery Appliance RA26フル・ラックは、最大**600 TB/時**の実効速度で実行される仮想フルバックアップをサポートし、14台のフル・ラック構成は最大**8ペタバイト/時**をサポートします。

2台のコンピューティング・サーバーと17台のストレージ・サーバーからなる単一のフル・ラックRecovery Appliance RA26は、最大60 TB/時の速度で継続的なバックアップおよびリストアを実行できます[3]。つまり、60 TB/時で変更データを受信して、***600 TB/時***の仮想バックアップに変換できます（変更率10 %と仮定）。
Recovery Applianceは、変更されたブロックだけを読み取り、転送し、処理するという独自の効率性を通じて、他のソリューションをはるかに上回る速度を達成します。他のソリューションでは、変更された部分を最初に判断する必要があります。

ラックを構成に追加すると、パフォーマンスと容量の両方が直線的に増強されます。14ラックのRecovery Appliance RA26は最大***8ペタバイト/時***の仮想フルバックアップ、800 TB/時の差分取得およびリストアを達成します。

[3] 省スペースの暗号化バックアップを使用した、Exadata X10M-EF（4つのDBノードと10個のストレージ・セル）とRA26（ストレージ・サーバー14台）による構成

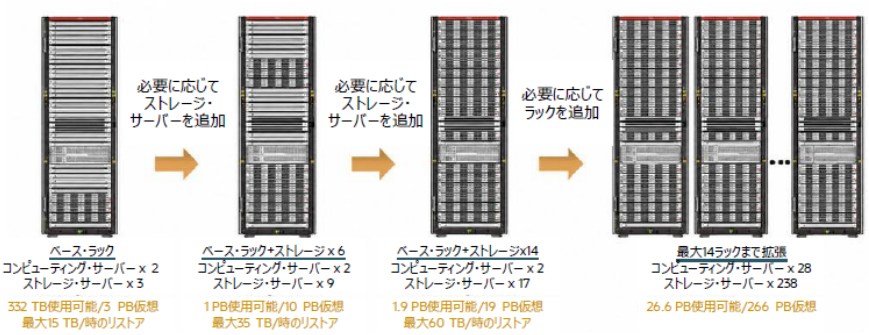

図3：Recovery Appliance RA26のスケールアウト・ラック構成

Recovery Applianceを100 Gb Top of Rack（ToR）スイッチで構成し、Exadata上にホストされている、保護データベースの専用バックアップ/リカバリ・ネットワークを構築できます。これにより、Recovery Applianceがデータセンターのバックアップ・ネットワークを共有する必要がなくなり、全体的なスループットが最適化されます。これは大量のデータベース・バックアップには特にメリットとなる可能性があります。このネットワーク構成は、以下に示すように、ExadataシステムをRecovery Applianceに設置された100 Gb ToRスイッチに接続することで実現します。

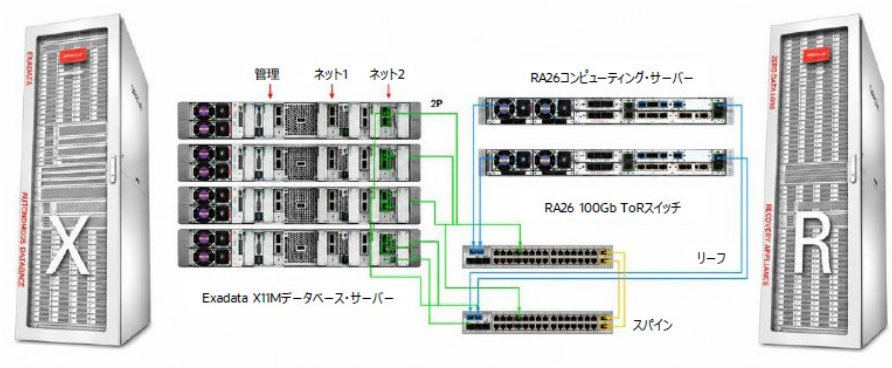

図4：Recovery Appliance RA26 100 Gb ToRスイッチ構成

ソフトウェア構成

Recovery Applianceの実行に必要なソフトウェアはすべて1つのソフトウェア・ライセンスに付属しています。

- バックアップ、リカバリ、およびレプリケーション
- メタデータおよびRecovery Managerのリカバリ・カタログ用の組込みOracle AI Database
- Recovery Appliance用のRecovery Managerバックアップ・モジュール
- ストレージ・ソフトウェア
- クラウド・ソフトウェアへのアーカイブ
- Amazon S3ソフトウェア向けのOracle Database Cloud Backup
- 暗号化および圧縮用のASOライセンスおよびACOライセンスの特別な使用

- Oracle Enterprise Managerによる監視および管理

通常のOracleライセンスと同様に、Recovery Applianceライセンスは新しいアプライアンスに完全に移転可能です。ライセンスの基準はストレージのテラバイト数ではなく、ストレージ・ディスク・ドライブ本数であるため、ディスク・ドライブがはるかに大容量でプロセッサが高速な新しいアプライアンスにおいても既存のライセンスを使用できます。

エンド・ツー・エンドのデータ保護管理

データ保護管理タスクは通常、データベース管理者、バックアップ管理者、ストレージ管理者などのITの役割に合わせて細分化された複数の管理領域に分断されています。したがって、Recovery Managerを使って開始されたバックアップが中間レイヤーで問題を起こさずに、最終的なバックアップ先に達したかどうかをDBAが判断することは多くの場合は困難です。

Recovery Applianceは、完全に自動化された統合データ保護管理でこの問題を解決します。

Oracle Enterprise Manager Cloud Controlによる統合管理

Recovery Applianceは、バックアップがRecovery Managerを使って開始されたときから、ディスク、クラウドに保存されるかリモート・データセンターの他のRecovery Applianceに複製されるまでのデータ保護ライフサイクルを、Oracle Enterprise Manager Cloud Controlを使ってエンド・ツー・エンドかつ一元的に表示します。すべてのバックアップの保存場所がRecovery Applianceによって追跡されるので、Recovery Managerのリストア操作とリカバリ操作によって、保存されている場所に関係なく最適なバックアップを取得できます。きめ細かいストレージとパフォーマンスのメトリックを含め、データ保護ライフサイクルへのこのレベルのエンド・ツー・エンドの可視性を提供できるのはRecovery Applianceだけです。

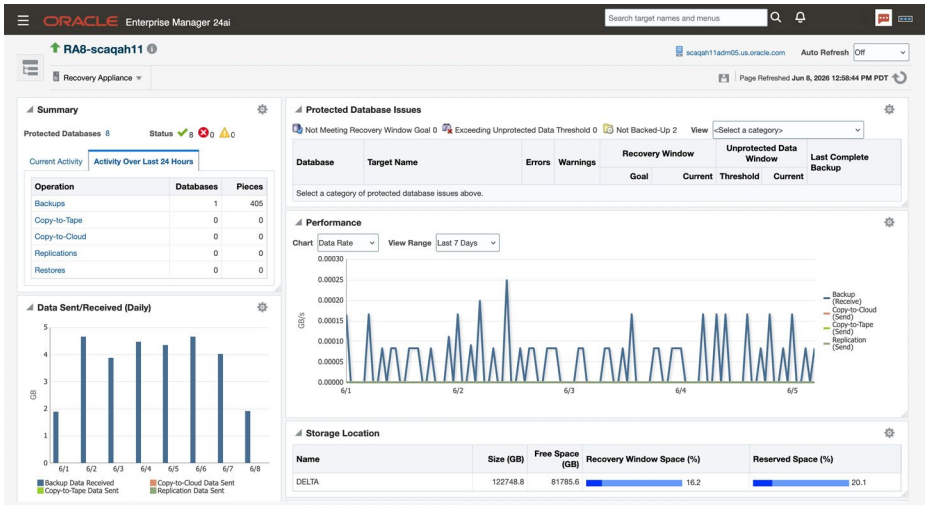

図5：一元化された保護管理 – ストレージとパフォーマンスのメトリック

Recovery Applianceは高度なストレージの監視とレポート機能を搭載して、データの増加に基づく容量の要件に加えて、現在と将来のスループットを効果的に管理します。Recovery Appliance管理下の各データベースに必要な領域の量は、そのバックアップ領域の使用履歴とリカバリ・ウィンドウ目標を基に予測的に計算されます。必要な領域はEnterprise

「企業は、従来の手法を使用する場合に起こりがちな停止時間やデータ損失なしで、主要ビジネス・アプリケーションの重要なデータをリアルタイムで保護する必要があります。
Zero Data Loss Recovery Applianceは、簡単なスケーリングによってデータベースを社内全体で保護し、厳格化するリカバリ・ポイント・オブジェクティブを満たす、シンプルでありながら強力なソリューションでこのニーズに対応します。」

IDC
ストレージ・プラクティス、プログラム・バイス・プレジデント
Laura Dubois氏

Managerでデータベースごとに明確に表示され、Recovery Applianceはすべてのデータベースに必要な総領域を、使用可能なストレージ合計のパーセンテージとして集計して、データ増加の対応から不確定要素を排除します。現在のデータの増加を基に、容量がいつ超過するかを知りたい場合は、Oracle Analytics Server（OAS）で利用可能なRecovery Appliance Capacity Reportさえ見れば、ストレージの使用率、7日、31日、365日の平均および最大スループットに関するサマリーと詳細、およびCPU、メモリ、IOPSの詳細を確認できます。また、必要な領域が使用可能な総領域の15 %以内（またはユーザーによる構成が可能な他のしきい値）である場合は、警告を生成できます。

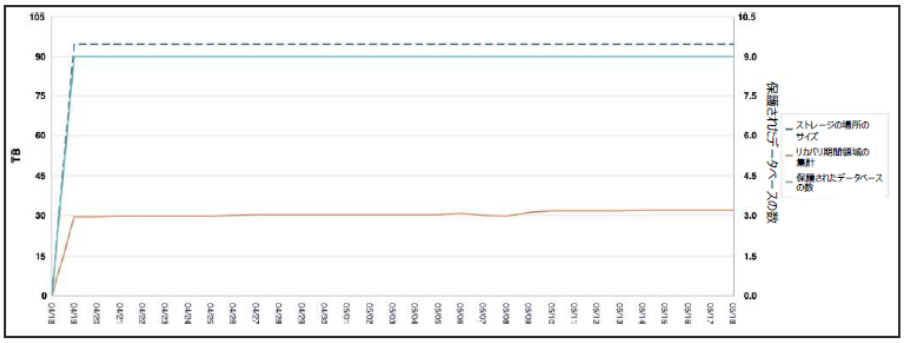

図6：容量計画 – 保護されたデータベースと領域の使用履歴

Oracle AI Databaseの保護に対応する統合管理の簡素性は、データベースをRecovery Appliance保護管理に効率的に追加できることからも明らかです。

- 新しいデータベースを追加する場合、Recovery Applianceの管理者はEnterprise Managerの"*Add Protected Database*"ウィザードを使って、データベースを適切な保護ポリシーに関連付け、データベースの資格証明を確立します。
- 次にデータベース管理者はデータベースのEnterprise ManagerのBackup Settingsページを使って、Recovery Applianceをバックアップ先に選択し、リアルタイムのREDO転送を任意で有効にして継続的にデータを保護します。

ランサムウェアからの回復力とリカバリ

近年、サイバー攻撃は、多様なアプローチとその破壊的な性質により、すべてのお客様にとって大きな懸念事項となっています。グローバル経済に対するマルウェアおよびランサムウェアの影響は膨大です。2025年の企業の損害額は570億ドルと推定され、2028年には1,250億ドルになると予測されています[4]。サイバー攻撃による企業の平均停止時間は、医療業界だけを見ても18日間を超え[5]、多くの場合は数週間、数か月にもわたっています。ミッション・クリティカルなデータベースにとって、データの損失やシステムの停止時間につながるこのような

[4] Global Ransomware Damage Cost Predictions In USD, 2025 to 2031, https://cybersecurityventures.com/wp-content/uploads/2023/11/RansomwareCost.pdf

[5] Average downtime caused by ransomware attacks in U.S. healthcare organizations from 2019 to 2023 YTD, Statista, https://www.statista.com/statistics/1422159/us-healthcare-ransomware-attacks-downtime-average-by-days

攻撃は、収益、業務、評判にとってマイナスになり、違約金を発生させる可能性もあるなど、ビジネス全体に広範囲な悪影響を与える可能性があります。

Recovery Applianceは本番データベースから障害が伝播しないように設計されているため、ランサムウェア攻撃が本番データベースを襲っても、アプライアンスが侵害されることはありません。これは、次のような主要なアーキテクチャ特性に起因します。

エンド・ツー・エンドのデータ検証

検証は、バックアップ・ライフサイクル全体を通して破損したバックアップ・データを検出することにおもな役割を果たしますが、ランサムウェア攻撃を受けたデータを検出するためにも等しく重要です。このアプライアンスによって、Oracleブロックの正確性とリカバリ可能性について、受信、オンディスク、レプリケーションのすべてのバックアップが検証されるため、マルウェアやランサムウェア攻撃の悪影響を受けたバックアップ・データがあれば検出、記録され、管理者にアラートが出されます。その後DBAと連携して、データベースをネットワークから切り離してさらに調査するなどのアクションを取ることができます。さらに、レプリケーションされたバックアップは、プライマリ・アプライアンスやその管理者が削除したり変更したりすることはできません。これらはレプリカ・アプライアンスによって独立的に検証および管理されます。したがって、プライマリ・アプライアンスに対する攻撃の影響からは保護されています。代替または補足的な保護戦略として、バックアップはセカンダリ・バックアップ・コピーのための安全な場所としてOracle Cloud Storageにアーカイブし、バックアップ暗号化キーについてはキー・ストアとしてOracle Key Vaultを使用することができます。すべてのバックアップはCloud Storageに暗号化されたまま保存され、リストア操作を実行するにはRecovery ApplianceとOracle Key Vaultにアクセスすることが必要になります。

不変バックアップ

不変バックアップは、バックアップ・データの不正な、または悪意のある、削除や変更から保護されて整合性を維持します。これは、歴史的には規制コンプライアンス要件を満たすために重要でしたが、最近では、マルウェアやランサムウェアの攻撃に対する追加の防御層として重要な役割を果たしています。Recovery Applianceは、規定のコンプライアンス保持期間内は不変であるバックアップを強制することができ、文書化されたインタフェースを使用した削除操作や保持期間の短縮は、これらのバックアップには影響を与えません。第2に、バックアップは政府や企業の措置により訴訟ホールドモードにすることができ、ホールドが解除されるまで無期限に保持されます。最後に、不変バックアップをOCIまたはZFS規制コンプライアンス・バケットにアーカイブすることで、より長期的な不変保持期間を設定できます。最終的に、このアーキテクチャは、ローカル・アプライアンスでのバックアップ作成から、DRサイトのレプリカ・アプライアンス、さらにクラウド・ストレージに至るまで、エンド・ツー・エンドの不変ソリューションを効果的に提供します。そのすべてはデータベース環境全体でEnterprise Managerにより一元的に管理および追跡されます。

職務の分離とクォーラム・ユーザーの承認

システムへのアクセスは、DBAとアプライアンス管理者のロール間の厳格な職務の分離によって制御されます。DBAには、特権データベースをバックアップおよびリカバリするためのVirtual Private Catalog（VPC）ユーザー・ロールが与えられるだけであり、アプライアンス上のバックアップへのアクセスや、その変更および削除はできません。Recovery Applianceの管理者は、システムを管理および監視するアクセス権のみを有し、保護されたデータベースをバックアップ、リカバリ、または変更することはできません。

さらに、アプライアンスは、指名された管理ユーザーを文書化されたインタフェースに制限し、SSHとOSへの直接アクセスを禁止します。これにより、汎用OSユーザー、データベース、その他のサービスが作成されてインストールされるのを防ぐことができます。ルート・アクセスは、クォーラム・ユーザーの承認によってのみ許可されます。つまり、他の2人の指名された管理者ユーザーが、特定の期間のルート・リクエストを承認する必要があります。

ネットワーク・アクセスの制限

ネットワーク・プロトコルに関しては、VPCユーザーは、SQL*Net経由でのみアプライアンスに接続できます。TLSは、SQL*Net経由で転送中のリアルタイムREDO、およびRecovery Appliance Backup Module（HTTPS）経由のRMANバックアップとリストアのトラフィックを暗号化するために有効にすることができます。保護されたデータベースからのそれ以外のアクセスは許可されません。さらに、アプライアンスはVLANタグ付きネットワークのサポートによりネットワークの分離を実施し、バックアップとリストアのトラフィックが、保護されたデータベースの特定のネットワーク・ゾーン間で完全に分離され、ルーティング不可になるようにします。このようにして、影響を受ける可能性のあるバックアップが、エンタープライズの他の部分に公開されることはなくなります。

Cyber Vault(サイバー・ボールト)の導入

バックアップを不正アクセスやランサムウェア攻撃のラテラル・ムーブメントからさらに分離するために、アプライアンスをCyber Vaultの場所に展開することができます。これにより、ボールトへのデータ送信は、本番の場所にあるアプライアンスからプライベート・レプリケーション・ネットワーク経由でしかできなくなります。このネットワークは"エア・ギャップ"として構成できます。つまり、通常はボールトへの接続は閉ざされ、アクセスはファイアウォール、ゲートウェイ、またはその他のネットワーク管理機能によって制御されます。ネットワークは、レプリケーションによる、ボールトと新しい本番バックアップとの定期的な同期のためにのみ開かれます。このアプライアンスは、効率的な永久増分バックアップを利用し、結果としてレプリケーションにも使用されるため、開かれている接続期間は非常に短く保たれ、悪意のある侵入の可能性は最小限に抑えられます。さらに、ボールト・アプライアンスの管理者資格証明やEnterprise Managerも、本番アプライアンスとDRアプライアンスの管理者とは完全に分離してセットアップできるため、ロケーション間の職務の分離層を構築できます。すべてのネットワークおよびレプリケーション・アクティビティは、ボールト内から開始できます。Cyber Vaultの導入について詳しくは、Zero Data Loss Recovery Applianceサイバー・セキュリティ・アーキテクチャの資料を参照してください。[6]

仮想エアギャップ

Recovery Applianceの仮想エアギャップ機能は、アプライアンス内でエアギャップの制御を一元化し、企業のITチームへの依存を減らすことで、セキュリティと業務効率を向上させます。RACLIコマンドの拡張により、管理者は本番アプライアンスとボールト・アプライアンス間のレプリケーションを正確に制御できるため、バックアップの同期期間に基づいてダウンストリームのネットワーク接続を開放、遮断、または制限できます。これによって、デプロイメントの簡素化、進行中の操作の効率化、セキュリティ体制の強化が実現します。詳細については、仮想エアギャップの概要についてのブログ[7]を参照してください。

関連製品

- Oracle Database 19c、23ai、26ai
- Oracle Cloud Infrastructure Storage
- Oracle ZFS Storage
- Enterprise Manager
- Oracle Database Zero Data Loss Autonomous Recovery Service

関連サービス

オラクルで利用できるサービスは次のとおりです。

- Oracle Advanced Customer Services
- Oracle Premier Support for Systems
- Oracle Platinum Services
- Oracle Consulting Services

6 Zero Data Loss Recovery Appliance Cyber Security Architecture, https://www.oracle.com/technetwork/database/availability/recovery-appliance-cyber-twp-6729502.pdf

[7] Introducing :Zero Data Loss Recovery Appliance Virtual Air Gap, https://blogs.oracle.com/maa/introducing-zdlra-virtual-air-gap-v-gap

優れたレジリエンス

アプライアンス自体も、従来のバックアップ・アプライアンスと比較して、ランサムウェア攻撃に対するはるかに優れたレジリエンス能力を持っています。Exadataハードウェアとストレージ上に構築されたOracle Engineered Systemとして、アプライアンスは、コンピューティング・サーバーとストレージ・サーバーの攻撃対象領域を削減する、高いレジリエンスを備えたアーキテクチャを継承しています。これには、強化されたパスワード・ポリシー、OSおよびDBユーザーの監査、ファイアウォールのサポート、Oracle ILOM（Integrated Lights Out Management）が含まれます。[8]

オラクルのTDEと統合した省スペースの暗号化バックアップ

オラクルの透過的データ暗号化（TDE）は、保存データの暗号化のためのオラクルの標準的な機能であり、データベース・カーネルに組み込まれています。これにより、操作とパフォーマンスへの影響を最小限に抑えながら、データベースを迂回する攻撃から保護します。また、業界最高レベルの暗号化をサポートしており、GDPR、CCPA、PCI-DSS、HIPAAなどの規制へのコンプライアンス要件を満たしています。TDEでは、データはデータベースのみを通じてアクセスでき、ディスク、バックアップ、またはエクスポートから直接読み取ることはできません。実際、Exadata Cloud@Customerでは、オラクルが管理するシステム（DOM0）に対するパッチ適用や保守などのアクティビティから顧客データを保護するために、TDEの使用が必須とされています。

TDEでは本番データからバックアップまでのデータを暗号化できますが、暗号化データはランダムな性質を持つため、暗号化は従来、ストレージベースの圧縮方式にマイナスの影響を与えてきました。顧客は、既存の保存要件を維持するためだけに2～3倍以上のバックアップ容量に投資するというジレンマに直面しています。おもに重複排除と圧縮に価値が置かれている市場のストレージ製品では、暗号化されたデータにとってはそれらの機能が意味を持たないため、データベース環境にとって全般的に適しているのかという疑問が生じます。

Recovery ApplianceはTDEデータ形式と統合されており、データベースの暗号化を保存時に維持する一方で、革新的な圧縮機能と永久増分バックアップ機能によって業界最高水準のバックアップ・ストレージの節約を実現します。省スペースの暗号化バックアップにより、汎用ストレージ・ソリューションと比較してバックアップ・ストレージを最大3分の1に削減でき、バックアップを2倍高速化できます。これは、お客様は*Recovery Appliance*により、ストレージ消費を最小限に抑えながら*TDE*を使用して本番からバックアップまでのライフサイクルを保護できるようになったという、データ保護業界における劇的な移行を表しています。

Zero Data Loss Recovery

データベース・サーバーが攻撃を受け、そのバックアップを別のサーバーにリカバリする必要がある場合、Recovery ApplianceのリアルタイムREDO転送によって、攻撃発生直前の最終トランザクションまでリカバリできます。これはランサムウェア攻撃では特に重要です。その攻撃では、犯人の要求に応じて金銭を渡したからといっても、必ずしもデータが元の状態で戻ってくるとは限りません。Recovery Applianceを使用すれば、要求された金銭を支払うことなく、データベースを分離された安全な場所にデータ損失なくリカバリができます。

[8] Oracle Exadata Security Guide：https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/index.html

SEC 17a-4（f）独立監査人による評価レポート

サイバー攻撃やランサムウェア攻撃の急増は、特に金融サービス部門において意識されており、それに伴い、電子記録の記録と保持に関する要件を定めたSEC規則17a-4（f）の適用にあらためて注目が集まっています。米国を拠点とする、あるいは米国での業務をサポートするすべての主要な金融機関は、次の5つのおもな要件で構成されるこの規制の対象となる可能性があります。

- 要求されている保持期間中のバックアップの上書きや消去を防ぐ（不変性を維持する）
- バックアップの品質と正確性を自動的に検証する
- バックアップを一意に保存する
- レポートやバックアップの検索用に、すぐに利用できるインデックスを維持する
- バックアップの複製コピーを保存する

大手の情報ガバナンス・コンサルティング会社であるCohasset Associatesは、Recovery Applianceの機能の独自評価を実施し、利用する顧客が上記の規制要件を適正に満たせることを確認しました。
レポート[9]では、各要件の詳細と、Recovery Applianceによって各要件をどのように満たすことができるかを示しています。これは金融サービス部門または同様の製品評価を必要とする他の規制業種を問わず、すべての顧客が利用できます。

パブリック・クラウドのOracle AI Database保護

お客様がクラウドへの移行を検討するときに、Recovery Applianceによって提供されるデータベース保護機能が、OCIおよびマルチクラウド（Azure、Google Cloud、AWS）上で実行するOracle Database Cloudサービス向けのZero Data Loss Autonomous Recovery Serviceとともに使用できるようになりました。Recovery Serviceによって、ランサムウェアのリスクを軽減するというビジネス・クリティカルなニーズ、運用効率の向上という財務要件、そしてクラウド・サービスのシンプルさを求めるユーザーの期待に応えることができます。詳細情報と参考資料については、発表に関するブログ[10]および製品Webサイト[11]を参照してください。

まとめ：次世代のインテリジェントなデータ保護

既存のデータ保護ソリューションはデータベースを、特定のデータの整合性、パフォーマンス、可用性の要件を持つトランザクション・システムとしてではなく、単にコピー対象の汎用ファイルとして扱っているので、重要なデータベースのニーズを満たすことができません。今日のレガシー・ソリューションでは、ビジネス・データは失われ、エンドユーザーが影響を受け、デプロイメントと管理が複雑で断片化します。

オラクルのZero Data Loss Recovery Applianceは高度なデータ保護テクノロジーをOracle AI Databaseと緊密に統合して、これらのオンプレミス環境の課題に対処します。

---

[9] Oracle Zero Data Loss Recovery Appliance SEC 17a-4(f) Compliance Assessment Report, Cohasset Associates：
https://www.oracle.com/a/ocom/docs/engineered-systems/recovery-appliance-compliance-assessment-report.pdf

[10] Introducing Oracle Database Zero Data Loss Autonomous Recovery Service
https://blogs.oracle.com/maa/post/introducing-recovery-service

[11] Oracle Database Zero Data Loss Autonomous Recovery Service：https://www.oracle.com/recoveryservice

また、クラウド・データベース向けに類似の機能を提供するZero Data Loss Autonomous Recovery Serviceの基盤の役割も果たします。Recovery Applianceは、次のことを実現する次世代のインテリジェントな手法でデータベース保護環境を再定義します。

- **データ損失の排除：**独自のデータベースとの統合により、REDOデータをRecovery Applianceに継続的に転送して、最新のトランザクションをリアルタイムで保護できるため、データを失うことなくデータベースをリストアできます。
- **災害からのデータ保護：**Recovery ApplianceはリモートRecovery Applianceにリアルタイムでデータを複製し、定期的にバックアップをクラウドにアーカイブすることで、ビジネス・データをサイト停止から保護できます。データベース・ブロックが継続的に検証されるので、転送または処理のどのステージでもデータ破損が排除されます。
- **本番環境への影響の排除：**Oracle AI Databaseに統合されたバックアップ・アルゴリズムは、変更されたデータだけをRecovery Applianceに送信して、本番データベースへの影響、I/Oトラフィック、ネットワーク負荷を最小限に抑えます。負荷の高いバックアップ処理はすべて、Recovery Applianceにオフロードされます。非生産的なバックアップ・ウィンドウは不要になり、ビジネス継続性が妨げられることはもうなくなります。
- **アーカイブ操作のオフロード：**Recovery Applianceはバックアップを低コストなクラウド・ストレージに直接アーカイブできるので、本番データベース・サーバーへの負荷が解消されます。アーカイブ操作は日中と夜間の両方の時間帯で実行できるので、リソースの使用率が向上します。
- **どの時点にもリストア可能：**アプライアンスに保存されたデータベースの変更データを使って、希望するどの時点でも仮想フルデータベースのコピーを効率的に作成できます。
- **クラウド規模の保護を提供：**単一のRecovery Applianceにより、データセンターまたは地域の数千ものデータベースのデータ保護要件に対処できます。停止時間を設けなくても、容量をペタバイト単位のストレージにシームレスに拡張できます。企業はポリシー・ベースの手法を使ってDatabase Protection as a Serviceを実装できるようになりました。その結果、管理者はエンタープライズ・データベース保護の状態をいつでもエンド・ツー・エンドで表示できます。
- **ランサムウェア攻撃からの防御：**アプライアンスは、本番データベースとは別の、独立して管理されるシステムであり、ランサムウェア攻撃に対するレジリエンスを考慮して設計されています。すべての受信、保存、送信されるバックアップ・データは、Oracleブロックの正確性について継続的に検証されます。これにより、侵害されたデータがあればすぐにアラートを受け取れます。不変保持期間は、データベース・レベルで設定して、重要なバックアップの悪意ある削除や変更を防ぐことができます。ユーザー・アクセスに関しては、DBAとアプライアンス管理者の間で職務の分離が厳格に実施されます。DBAは、バックアップ/リストアのみを行うことができ、バックアップの削除やアプライアンスの変更にはアクセスできません。管理者はその逆で、アプライアンスを管理しますが、データベースのバックアップ/リストアを行うアクセス権限はありません。さらに、複製されたバックアップはプライマリ・バックアップから独立して管理および検証されるため、プライマリ・アプライアンスへの攻撃により悪影響を受けたデータの影響を受けることはありません。システム・アクセス自体は、

日常業務へのアクセスを制限し、ルート・アクセスを禁止する、指名された管理者のユーザー・モデルによって保護および記録されます。バックアップ・データをさらに分離するために、アプライアンスはエア・ギャップのあるCyber Vaultの場所に、個別のユーザー・アクセス資格証明とともに展開することができ、必要な場合には、永久増分レプリケーションによって本番バックアップと効率的に同期させることができます。

このアプライアンスは、業界をリードするExadataプラットフォーム上に構築され、強固なパスワード・ポリシー、きめ細かなアクセス制御、包括的な監査、セキュアな完全自動管理を実現することで、レジリエンスと監視機能を提供します。

Oracle on Oracleのもう1つの利点は、Recovery Applianceのバックアップ Oracle Transparent Data Encryption（TDE）と統合されている点です。ここではデータベースネイティブの暗号化が維持され、バックアップ・サイクル全体を通してバックアップ領域の消費は最小限で済みます。これは、TDEに対応した革新的なバックアップ圧縮および永久増分戦略によって実現し、他の汎用バックアップ・ソリューションと比較して3倍以上の領域が節約されます。

最後に、本番データベース自体が攻撃によって侵害された場合、Recovery Applianceを使用して、攻撃時点までのすべてのトランザクションを含むすべてのデータを、別の安全な場所にリストアできます。オラクルのデータ損失ゼロの保護ソリューションについて詳しくは、Oracle Database Protection and Ransomware ResiliencyのWebサイトを参照してください。

Recovery Appliance RA26, RA26-Zサーバー・ハードウェア

サーバー・タイプ	ストレージ	ネットワーク

**RA26
コンピューティング・サーバー
（ラックあたり2台）**
	2 x NVMeフラッシュSSD
	（ホットスワップ対応）
		• 2 x デュアル・ポート10/25 GbイーサネットSFP28
		  ○ 2 x 10/25 Gb光（インジェスト）
		  ○ 2 x 10/25 Gb光（レプリケーション）
		• 2 x デュアル・ポート100 GbイーサネットQSFP28
		  ○ 2 x 100 Gb光（インジェスト）
		  ○ 2 x 100 Gb光（レプリケーション）
		• 1 x クアッド・ポート10 GbイーサネットRJ45
		  ○ 2 x 10 Gb銅（インジェスト）
		  ○ 2 x 10 Gb銅（レプリケーション）
		• 2 x 100 Gb QSFP28 RoCEファブリック・ポート
		• 1 x 1 Gbイーサネット銅ポート（管理）
		• 1 x ILOMイーサネットポート
		• 2 x 10 Gbポート、2 x 25 Gbポート、または2 x 100 Gbポート（最大）、インジェスト・ネットワーク用
		• 2 x 10 Gbポート、2 x 25 Gbポート、または2 x 100 Gbポート（最大）、レプリケーション・ネットワーク用

RA26 ストレージ・サーバー **RA26-Z ストレージ・サーバー**	12 x 26 TB 7,200 RPM ディスク 2 x NVMeフラッシュ・ アクセラレーション・カード 6 x 26 TB 7,200 RPM ディスク 2 x NVMeフラッシュ・ アクセラレーション・カード	• 2 x 100 Gb QSFP28 RoCEファブリック・ポート • 1 x 1 Gbイーサネット銅ポート（管理） • 1 x ILOMイーサネットポート

[1]すべてのサーバーに、冗長化されたホットスワップ対応ファンと電源が組み込まれています。

Recovery Appliance RA26の構成

ラック・サイズ	コンピューティング・サーバー	ストレージ・サーバー	使用可能容量（標準冗長性）	使用可能容量（高冗長性）
ベース・ラック	コンピューティング・サーバー x 2	ストレージ・サーバー x 3	332 TB	213 TB
+ストレージ・サーバー	非該当	最大14台の追加ストレージ・サーバー	ストレージ・サーバーあたり112 TB	ストレージ・サーバーあたり72 TB

[1]各ラックの高さは42 RU（ラック・ユニット）で、冗長化された配電ユニット（PDU）2台、36ポート100 Gb/秒RoCEスイッチ2個および48ポート管理イーサネット・スイッチ1個を収容します。
単一ラックに最大17台のストレージ・サーバーを搭載可能です。
フル・ラックの使用可能容量：

- 標準冗長性：1.9 PB
- 高冗長性：1.2 PB

Recovery Appliance RA26-Zの構成

ラック・サイズ	コンピューティング・サーバー	ストレージ・サーバー	使用可能容量（標準冗長性）	使用可能容量（高冗長性）
ベース・ラック	コンピューティング・サーバー x 2	ストレージ・サーバー x 3	164 TB	104 TB
+ストレージ・サーバー	非該当	最大14台の追加ストレージ・サーバー	ストレージ・サーバーあたり56 TB	ストレージ・サーバーあたり36 TB

Recovery Appliance RA26ストレージ・サーバーの環境仕様

メトリック	仕様
高さ	86.9 mm（3.42インチ）
幅	445.0 mm（17.52インチ）
奥行き	759.0 mm（29.88インチ）
騒音（動作時）	8.1 B
重量	31.3 kg（69ポンド）
最大消費電力	0.5 kW（0.5 kVA）
標準消費電力[1]	0.4 kW（0.4 kVA）
最大使用時の冷却能力	1,825 BTU/時
	1,926 kJ/時
標準使用時の冷却能力	1,278 BTU/時
	1,348 kJ/時
最大使用時のエアフロー[2]	85 CFM

標準使用時のエアフロー[2]	59 CFM

動作時温度/湿度：5 ºC～32 ºC（41 ºF～89.6 ºF）、10 %～90 %相対湿度、結露なし
動作時高度：最大3,048 m（高度900 m以上では300 m上昇するごとに最大周囲温度が1 °C低下）
[1] 標準消費電力は、アプリケーションの負荷によって変わります。
[2] エアフローは前面から背面へと流れる必要があります

Recovery Appliance RA26-Zストレージ・サーバーの環境仕様

メトリック	仕様
高さ	86.9 mm（3.42インチ）
幅	445.0 mm（17.52インチ）
奥行き	759.0 mm（29.88インチ）
騒音（動作時）	7.5 B
重量	28.4 kg（62.7ポンド）
最大消費電力	0.5 kW（0.5 kVA）
標準消費電力[1]	0.3 kW（0.3 kVA）
最大使用時の冷却能力	1,629 BTU/時
	1,719 kJ/時
標準使用時の冷却能力	1,140 BTU/時
	1,203 kJ/時
最大使用時のエアフロー[2]	75 CFM
標準使用時のエアフロー[2]	53 CFM

動作時温度/湿度：5 ºC～32 ºC（41 ºF～89.6 ºF）、10 %～90 %相対湿度、結露なし
動作時高度：最大3,048 m（高度900 m以上では300 m上昇するごとに最大周囲温度が1 °C低下）
[1] 標準消費電力は、アプリケーションの負荷によって変わります。
[2] エアフローは前面から背面へと流れる必要があります

Recovery Appliance RA26の環境仕様

メトリック	ベース・ラック	フル・ラック
高さ	2,000 mm（78.74インチ）	
幅	601 mm（23.66インチ）	
奥行き	1,197 mm（47.13インチ）	
騒音（動作時）	9.1 B	9.5 B
重量	418.6 kg（922.8ポンド）	934.4 kg（2,060.0ポンド）
最大消費電力	4.0 kW（4.1 kVA）	11.5 kW（11.8 kVA）
標準消費電力[1]	2.8 kW（2.9 kVA）	8.1 kW（8.2 kVA）
最大使用時の冷却能力	13,782 BTU/時（14,540 kJ/時）	39,339 BTU/時（41,502 kJ/時）
標準使用時の冷却能力	9,647 BTU/時（10,178 kJ/時）	27,537 BTU/時（29,052 kJ/時）
最大使用時のエアフロー[2]	638 CFM	1,821 CFM
標準使用時のエアフロー[2]	447 CFM	1,275 CFM

動作時温度/湿度：5 ºC～32 ºC（41 ºF～89.6 ºF）、10 %～90 %相対湿度、結露なし
動作時高度：最大3,048 m（高度900 m以上では300 m上昇するごとに最大周囲温度が1 °C低下）
[1]標準消費電力は、アプリケーションの負荷によって変わります。
[2]エアフローは前面から背面へと流れる必要があります。

Recovery Appliance RA26-Zの環境仕様

メトリック	ベース・ラック	フル・ラック
高さ	2,000 mm（78.74インチ）	
幅	601 mm（23.66インチ）	
奥行き	1,197 mm（47.13インチ）	
騒音（動作時）	9.1 B	9.5 B
重量	410.0 kg（903.9ポンド）	885.8 kg（1,952.9ポンド）
最大消費電力	3.9 kW（3.9 kVA）	10.5 kW（10.8 kVA）
標準消費電力[1]	2.7 kW（2.8 kVA）	7.4 kW（7.5 kVA）
最大使用時の冷却能力	13,192 BTU/時（13,918 kJ/時）	35,997 BTU/時（37,977 kJ/時）
標準使用時の冷却能力	9,234 BTU/時（9,742 kJ/時）	25,198 BTU/時（26,584 kJ/時）
最大使用時のエアフロー[2]	611 CFM	1,667 CFM
標準使用時のエアフロー[2]	428 CFM	1,167 CFM

動作時温度/湿度：5 ºC～32 ºC（41 ºF～89.6 ºF）、10 %～90 %相対湿度、結露なし
動作時高度：最大3,048 m（高度900 m以上では300 m上昇するごとに最大周囲温度が1 °C低下）
[1]標準消費電力は、アプリケーションの負荷によって変わります。
[2]エアフローは前面から背面へと流れる必要があります。

Recovery Appliance RA26：準拠規格と認定規格

準拠規格[1, 2, 3]	**安全性：**	UL/CSA 60950-1、EN 60950-1、IEC 60950-1 CB Scheme（各国の規定に準拠） UL/CSA 62368-1、EN 62368-1、IEC 62368-1 CB Scheme（各国の規定に準拠）
	EMC	
	排出量：	FCC CFR 47 Part 15、ICES-003、EN55032、KN32、EN61000-3-11、EN61000-3-12
	イミュニティ：	EN55024、KN35
認定規格[2, 3]	NRTL（北米）、CE（欧州連合）、International CB Scheme、HSE Exemption（インド）、BSMI（台湾）、EAC（ロシアを含むEAEU）、KC（韓国）、RCM（オーストラリア）、VCCI（日本）、UKCA（イギリス）	
EU指令[3]	2014/35/EU 低電圧指令、2014/30/EU EMC指令、2011/65/EU RoHS指令、2012/19/EU WEEE指令	

[1] 言及した準拠規格と認定規格はすべて、最新の正式版です。詳細については、販売担当者にお問い合わせください。
[2] その他の国の準拠規格/認定規格が適用される場合もあります。
[3] 準拠規格や認定規格の遵守は、シェルフレベルのシステムのみで実現されている場合があります。

Recovery Applianceサポート・サービス

- ハードウェア保証：1年間、通常営業時間内（月～金の午前8時から午後5時まで）に4時間のWeb/電話対応、2営業日のオンサイト対応/パーツ交換
- Oracle Premier Support for Systems：Oracle Linuxのサポートと、24時間365日のサポート、2時間のオンサイト・ハードウェア・サービス対応（サービス・センターまでの距離による）
- Oracle Premier Support for Operating Systems
- Oracle Customer Data and Device Retention
- システム設置サービス
- ソフトウェア構成サービス
- Oracle Platinum Services
- Business Critical Service for Systems
- システム・アップグレード・サポート・サービス（ハードウェアの取り付けとソフトウェアの構成を含む）
- Oracle Auto Service Request（Oracle ASR）

お客様が用意したイーサネット・スイッチをRecovery Applianceにインストールするオプション

各Recovery Applianceラックの上部には2Uサイズの空きがあり、お客様は、独自のクライアント・ネットワークのイーサネット・スイッチを、別個のラックではなくアプライアンス・ラックにインストールできます。設置スペース、電力、冷却に関する一部の制限が適用されます。

Connect with us

+1.800.ORACLE1までご連絡いただくか、**oracle.com**をご覧ください。北米以外の地域では、**oracle.com/contact**で最寄りの営業所をご確認いただけます。

blogs.oracle.com facebook.com/oracle twitter.com/oracle